# FAMILIES OF CURVES OVER ANY FINITE FIELD WITH A CLASS NUMBER GREATER THAN THE LACHAUD - MARTIN-DESCHAMPS BOUNDS

STÉPHANE BALLET AND ROBERT ROLLAND

Abstract. We study and explicitly construct some families of asymptotically exact sequences of algebraic function fields. It turns out that these families have an asymptotical class number widely greater than the general Lachaud - Martin-Deschamps bounds. We emphasize that we obtain asymptotically exact sequences of algebraic function fields over any finite field $\mathbb{F}_q$, in particular when $q$ is not a square and that these sequences are dense towers.

## 1. Introduction

The algebraic properties of algebraic function fields defined over a finite field is somehow reflected by their numerical properties, namely their numerical invariants such as the number of places of degree one over a given ground field extension, the number of classes of its Picard group, the number of effective divisors of a given degree and so on. When, for a given finite ground field, the sequence of the genus of a sequence of algebraic function fields tends to infinity, there exist asymptotic formulae for different numerical invariants. In [10], Tsfasman generalizes some results on the number of rational points on the curves (due to Drinfeld-Vladut [13], and Serre [8]) and on its Jacobian (due to Vladut [12], Rosemblum and Tsfasman [7]). He gives a formula for the asymptotic number of divisors, and some estimates for the number of points in the Poincaré filtration. In this aim, he introduced the notion of asymptotically exact family of curves defined over a finite field. Let us recall this notion in the language of algebraic function fields.

**Definition 1.1.** *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ be a sequence of algebraic function fields $F_k/\mathbb{F}_q$ defined over $\mathbb{F}_q$ of genus $g_k = g(F_k/\mathbb{F}_q)$. We suppose that the sequence of the genus $g_k$ is an increasing sequence*

*Date*: June 30, 2009.
2000 *Mathematics Subject Classification.* Primary 12E20; Secondary 14H05.
*Key words and phrases.* finite field, function field, asymptotically exact sequence of functions fields, class number, tower of function field.

*growing to infinity. The sequence $\mathcal{F}/\mathbb{F}_q$ is said to be asymptotically exact if for all $m \geq 1$ the following limit exists:*

$$\beta_m(\mathcal{F}/\mathbb{F}_q) = \lim_{k\rightarrow+\infty} \frac{B_m(F_k/\mathbb{F}_q)}{g_k}$$

*where $B_m(F_k/\mathbb{F}_q)$ is the number of places of degree $m$ on $F_k/\mathbb{F}_q$.*

*The sequence $(\beta_1, \beta_2, ...., \beta_m, ...)$ is called the type of the aymptotically exact sequence $\mathcal{F}/\mathbb{F}_q$.*

Tsfasman and Vladut in [11] made use of this notion to obtain new general results on the asymptotic properties of zeta functions of curves.

Note that a simple diagonal argument proves that each sequence of algebraic function fields of growing genus, defined over a finite field admits an asymptotically exact subsequence. Unfortunately, this extraction method is not really suitable for the two following reasons. Firstly, in general we do not obtain by this process an explicit asymptotically exact sequence of algebraic function fields defined over an arbitrary finite field, in particular when $q$ is not a square. Secondely, the extracted sequence is not a sufficiently dense asymptotically exact sequence of algebraic function fields defined over an arbitrary finite field, namely with a control on the growing of the genus. Let us define the notion of density of a family of algebraic function fields defined over a finite field of growing genus:

**Definition 1.2.** *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq1}$ be a sequence of algebraic function fields $F_k/\mathbb{F}_q$ of genus $g_k = g(F_k/\mathbb{F}_q)$, defined over $\mathbb{F}_q$. We suppose that the sequence of genus $g_k$ is an increasing sequence growing to infinity. Then, the density of the sequence $\mathcal{F}/\mathbb{F}_q$ is*

$$d(\mathcal{F}/\mathbb{F}_q) = \liminf_{k\rightarrow+\infty} \frac{g_k}{g_{k+1}}.$$

A high density can be a useful property in some applications of sequences or towers of function fields. Until now, no explicit examples of dense asymptotically exact sequences $\mathcal{F}/\mathbb{F}_q$ have been pointed out unless for the case $q$ square and type $(\sqrt{q}-1, 0, \cdots)$.

In section 2, we show that we can construct general families, of asymptotically exact sequences of algebraic function fields defined over an arbitrary finite field $\mathbb{F}_q$ of type $(0, ..., \frac{1}{r}(q^{\frac{r}{2}}-1), 0, ..., 0, ...)$ where $r$ is an integer $\geq 1$. In this aim, we prove the main theorem 2.2 on sequences of algebraic function fields such that $\beta_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q-1)$. We study for these general families the behaviour of the class number $h_k$, and we compare our estimation to the general known bounds of

Lachaud - Martin-Deschamps. We also study the number of effective divisors.

Next, in section 3, we construct explicit examples of very dense asymptotically exact sequences defined over an arbitrary finite field $\mathbb{F}_q$. For this purpose we use towers of algebraic function fields having for constant field extension of a given degree $r$ the densified towers of Garcia-Stichtenoth (cf. [5] and [1]). In particular, we construct an asymptotically exact tower of algebraic function fields defined over $\mathbb{F}_2$ with a maximal density . This tower has an interesting application in the theory of algebraic complexity [4].

## 2. General results

2.1. **New families of asymptotically exact sequences.** First, let us recall certain asymptotic results. Let us first give the following result obtained by Tsfasman in [10]:

**Proposition 2.1.** *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ be a sequence of algebraic function fields of increasing genus $g_k$ growing to infinity. Let $f$ be a function from $\mathbb{N}$ to $\mathbb{N}$ such that $f(g_k) = o(log(g_k))$. Then*

$$\limsup_{g_k\to+\infty} \frac{1}{g_k}\sum_{m=1}^{f(g_k)} \frac{mB_m(F_k)}{q^{m/2}-1} \leq 1. \tag{1}$$

Using this proposition we can obtain the following main theorem:

**Theorem 2.2.** *Let $r$ be an integer $\geq 1$ and $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ be a sequence of algebraic function fields of increasing genus defined over $\mathbb{F}_q$ such that $\beta_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q^{\frac{r}{2}}-1)$. Then $\beta_m(\mathcal{F}/\mathbb{F}_q) = 0$ for any integer $m \neq r$. In particular, the sequence $\mathcal{F}/\mathbb{F}_q$ is asymptotically exact.*

*Proof.* Let us fix $m \neq r$ and let us prove that $\beta_m(\mathcal{F}/\mathbb{F}_q) = 0$. We use Proposition 2.1 with the constant function $f(g) = s = \max(m, r)$. Then we get

$$\limsup_{k\to+\infty} \frac{1}{g_k}\sum_{j=1}^{s} \frac{jB_j(F_k)}{q^j-1} \leq 1.$$

But by hypothesis

$$\limsup_{k\to+\infty} \frac{rB_r(F_k)}{g_k(q^{\frac{r}{2}}-1)} = \lim_{k\to+\infty} \frac{rB_r(F_k)}{g_k(q^{\frac{r}{2}}-1)} = 1.$$

Then

$$\limsup_{g_k\to+\infty} \frac{1}{g_k}\sum_{1\leq j\leq s; j\neq r} \frac{jB_j(F_k)}{q^j-1} = \lim_{g_k\to+\infty} \frac{1}{g_k}\sum_{1\leq j\leq s; j\neq r} \frac{jB_j(F_k)}{q^j-1} = 0.$$

But
$$\frac{B_m(F_k)}{g_k} \leq \frac{(q^m-1)}{m}\left(\frac{1}{g_k}\sum_{1\leq j\leq s; j\neq r}\frac{jB_j(F_k)}{q^j-1}\right).$$
Hence
$$\lim_{g_k\rightarrow+\infty}\frac{B_m(F_k)}{g_k}=0.$$
□

Note that for any $k$ the following holds:
$$B_1(F_k/\mathbb{F}_{q^r})=\sum_{i|r} iB_i(F_k/\mathbb{F}_q).$$
Then if $\beta_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q^{\frac{r}{2}}-1)$, by Theorem 2.2 we conclude that $\beta_1(\mathcal{F}/\mathbb{F}_{q^r})$ exists and that
$$\beta_1(\mathcal{F}/\mathbb{F}_{q^r})=(q^{\frac{r}{2}}-1).$$
In particular the sequence $\mathcal{F}/\mathbb{F}_{q^r}$ reaches the Drinfeld-Vladut bound and consequently $q^r$ is a square.

If $\beta_1(\mathcal{F}/\mathbb{F}_{q^r})$ exists then it does not necessarily imply that $\beta_r(\mathcal{F}/\mathbb{F}_q)$ exists but only that $\lim_{k\rightarrow+\infty}\frac{\sum_{m|r} mB_m(F_k/\mathbb{F}_q)}{g_k}$ exists. In fact, this converse depends on the defining equations of the algebraic function fields $F_k/\mathbb{F}_q$.

Now, let us give a simple consequence of Theorem 2.2.

**Proposition 2.3.** *Let $r$ and $i$ be integers $\geq 1$ such that $i$ divides $r$. Suppose that $\mathcal{F}/\mathbb{F}_q=(F_k/\mathbb{F}_q)_{k\geq 1}$ is an asymptotically exact sequence of algebraic function fields defined over $\mathbb{F}_q$ of type $(\beta_1=0,\ldots,\beta_{r-1}=0, \beta_r=\frac{1}{r}(q^{\frac{r}{2}}-1), \beta_{r+1}=0,\ldots)$. Then the sequence $\mathcal{F}/\mathbb{F}_{q^i}=(F_k/\mathbb{F}_{q^i})_{k\geq 1}$ of algebraic function field defined over $\mathbb{F}_{q^i}$ is asymptotically exact of type $(\beta_1=0,..,\beta_{\frac{r}{i}-1}=0,\beta_{\frac{r}{i}}=\frac{i}{r}(q^{\frac{r}{2}}-1),\beta_{\frac{r}{i}+1}=0,\ldots)$.*

*Proof.* Let us remark that by [9, Lemma V.1.9, p. 163], if $P$ is a place of degree $r'$ of $F/\mathbb{F}_q$, there are $\gcd((r',i))$ places of degree $\frac{r'}{\gcd(r',i)}$ over $P$ in the extension $F/\mathbb{F}_{q^i}$. As we are interested by the places of degree $r/i$ in $F/\mathbb{F}_{q^i}$, let us introduce the set
$$S=\{r'; r\ \gcd(r',i)=i\,r'\}=\{r'; \mathrm{lcm}\,(r',i)=r\}.$$
Then,
$$B_{r/i}(F/\mathbb{F}_{q^i})=\sum_{r'\in S}\frac{ir'}{r}B_{r'}(F/\mathbb{F}_q).$$
We know that all the $\beta_j(F/\mathbb{F}_q)=0$ but $\beta_r(F/\mathbb{F}_q)=\frac{1}{r}(q^{\frac{r}{2}}-1)$. Then
$$\beta_{r/i}(F/\mathbb{F}_{q^i})=i\beta_r(F/\mathbb{F}_q),$$

$$\beta_{r/i}(F/\mathbb{F}_{q^i}) = \frac{i}{r}\left(q^{\frac{r}{2}} - 1\right).$$

□

2.2. **Number of points of the Jacobian.** Now, we are interested by the Jacobian cardinality of the asymptotically exact sequences $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ of type $(0,..,0,\frac{1}{r}(q^{\frac{r}{2}}-1),0,...,0)$.

Let us denote by $h_k = h_k(F_k/\mathbb{F}_q)$ the class number of the algebraic function field $F_k/\mathbb{F}_q$. Let us consider the following quantities introduced by Tsfasman in [10]:

$$H_{inf} = H_{inf}(\mathcal{F}/\mathbb{F}_q) = \liminf_{k\to+\infty} \frac{1}{g_k}\log h_k$$

$$H_{sup} = H_{sup}(\mathcal{F}/\mathbb{F}_q) = \limsup_{k\to+\infty} \frac{1}{g_k}\log h_k$$

If they coincides, we just write:

$$H = H(\mathcal{F}/\mathbb{F}_q) = \lim_{k\to+\infty} \frac{1}{g_k}\log h_k = H_{inf} = H_{sup}.$$

Then under the assumptions of the previous section, we obtain the following result on the sequence of class numbers of these families of algebraic function fields:

**Theorem 2.4.** *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ be a sequence of algebraic function fields of increasing genus defined over $\mathbb{F}_q$ such that $\beta_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q^{\frac{r}{2}}-1)$ where $r$ is an integer. Then, the limit $H$ exists and we have:*

$$H = H(\mathcal{F}/\mathbb{F}_q) = \lim_{k\to+\infty} \frac{1}{g_k}\log h_k = \log \frac{q^{q^{\frac{r}{2}}}}{(q^r-1)^{\frac{1}{r}(q^{\frac{r}{2}}-1)}}.$$

*Proof.* By Corollary 1 in [10], we know that for any asymptotically exact family of algebraic function fields defined over $\mathbb{F}_q$, the limit $H$ exists and $H = \lim_{k\to+\infty}\frac{1}{g_k}\log h_k = \log q + \sum_{m=1}^{\infty}\beta_m.\log\frac{q^m}{q^m-1}$. Hence, the result follows from Theorem 2.2. □

**Corollary 2.5.** *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ be a sequence of algebraic function fields of increasing genus defined over $\mathbb{F}_q$ such that $\beta_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q^{\frac{r}{2}}-1)$ where $r$ is an integer. Then there exists an integer $k_0$ such that for any integer $k \geq k_0$,*

$$h_k > q^{g_k}$$

*Proof.* By Theorem 2.4, we have $\lim_{k\to+\infty}(h_k)^{\frac{1}{g_k}} = \frac{q^{q^{\frac{r}{2}}}}{(q^r-1)^{\frac{1}{r}(q^{\frac{r}{2}}-1)}}$. But

$$\frac{q^{q^{\frac{r}{2}}}}{(q^r-1)^{\frac{1}{r}(q^{\frac{r}{2}}-1)}} > \frac{q^{q^{\frac{r}{2}}}}{(q^r)^{\frac{1}{r}(q^{\frac{r}{2}}-1)}} = q.$$

Hence, for a sufficiently large $k_0$, we have for $k \geq k_0$ the following inequality

$$(h_k)^{\frac{1}{g_k}} > q.$$

□

Let us compare this estimation of $h_k$ to the general lower bounds given by G. Lachaud and M. Martin-Deschamps in [6].

**Theorem 2.6** (Lachaud - Martin-Deschamps bounds)**.** *Let $X$ be a projective irreducible and non-singular algebraic curve defined over the finite field $\mathbb{F}_q$ of genus $g$. Let $J_X$ be the jacobian of $X$ and $h$ the class number $h = |J_X(\mathbb{F}_q)|$. Then*

(1) $h \geq L_1 = q^{g-1}\frac{(q-1)^2}{(q+1)(g+1)}$,
(2) $h \geq L_2 = \left(\sqrt{q}-1\right)^2 \frac{g^{g-1}-1}{g}\frac{|X(\mathbb{F}_q)|+q-1}{q-1}$,,
(3) *if $g > \sqrt{q}/2$ and if $B_1(X/\mathbb{F}_q) \geq 1$, then the following holds:* $h \geq L_3 = (q^g-1)\frac{q-1}{q+g+gq}$.

Then we can prove that for a family of algebraic function fields satisfying the conditions of Corollary 2.5, the class numbers $h_k$ greatly exceeds the bounds $L_i$. More precisely

**Proposition 2.7.** *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ be a sequence of algebraic function fields of increasing genus defined over $\mathbb{F}_q$ such that $\beta_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q^{\frac{r}{2}}-1)$ where $r$ is an integer. Then*

(1) *for $i = 1, 3$*

$$lim_{k\to+\infty}\frac{h_k}{L_i} = +\infty,$$

(2) *for $i = 2$ the following holds:*
   (a) *if r>1 then*

$$lim_{k\to+\infty}\frac{h_k}{L_2} = +\infty,$$

   (b) *if r=1 then*

$$\frac{h_k}{L_2} \geq 2,$$

*Proof.* (1) case $i = 1$: the following holds

$$L_1 = q^{g_k-1}\frac{(q-1)^2}{(q+1)(g_k+1)} = q^{g_k}\frac{(q-1)^2}{q(q+1)(g_k+1)} < \frac{q^{g_k}}{(g_k+1)},$$

so, using the previous corollary 2.5, we conclude that for $k$ large

$$\frac{h_k}{L_1} > g_k$$

and consequently

$$\lim_{k\to+\infty}\frac{h_k}{L_1} = +\infty;$$

(2) case $i = 2$:
   (a) case $r = 1$: in this case, we just bound the number of rational points by the Weil bound. More precisely

$$L_2 = (q+1-2\sqrt{q})\ \frac{q^{g_k-1}-1}{g_k}\ \frac{B_1(F_k/\mathbb{F}_q)+q-1}{q-1} \leq$$
$$(q+1-2\sqrt{q})\ \frac{q^{g_k-1}-1}{g_k}\ \frac{2q+2g_k\sqrt{q}}{q-1} <$$
$$2\,\frac{q+1-2\sqrt{q}}{(q-1)\sqrt{q}}q^{g_k}\left(1+\frac{\sqrt{q}}{g_k}\right);$$

   but for all $q \geq 2$

$$2\,\frac{q+1-2\sqrt{q}}{(q-1)\sqrt{q}} < 0.4,$$

   then

$$L_2 < 0.4\left(1+\frac{\sqrt{q}}{g_k}\right)q^{g_k},$$

   hence

$$\frac{h_k}{L_2} > 2.5\,\frac{g_k}{g_k+\sqrt{q}}$$

   which gives the resul;
   (b) case $r > 1$: in this case we know that

$$\lim_{k\to+\infty}\frac{B_1(F_k/\mathbb{F}_q)}{g_k} = \beta_1(\mathcal{F}/\mathbb{F}_q) = 0.$$

   But

$$L_2 < \frac{q+1-2\sqrt{q}}{(q-1)q}q^{g_k}\frac{B_1(F_k/\mathbb{F}_q)+q-1}{g_k}.$$

   Then

$$\frac{h_k}{L_2} > \frac{(q-1)q}{q+1-2\sqrt{q}}\ \frac{g_k}{B_1(F_k/\mathbb{F}_q)+q-1}.$$

We know that

$$\lim_{k \to +\infty} \frac{g_k}{B_1(F_k/\mathbb{F}_q) + q - 1} = +\infty,$$

then

$$\lim_{k \to +\infty} \frac{h_k}{L_2} = +\infty.$$

(3) case $i = 3$:

$$L_3 = (q^g - 1)\frac{q-1}{q+g+gq} < \frac{q^{g_k}}{g_k},$$

then for $k$ large

$$\frac{h_k}{L_3} > g_k$$

and consequently

$$\lim_{k \to +\infty} \frac{h_k}{L_1} = +\infty.$$

□

As we see, if $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k \geq 1}$ satisfies the assumptions of Theorem 2.4, we have $h_k > q^{g_k} > q^{g_k - 1}\frac{(q-1)^2}{(q+1)g_k}$ for $k \geq k_0$ sufficiently large. In fact, the value $k_0$ depends at least on the values of $r$ and $q$ and we can not know anything about this value in the general case.

2.3. **Number of effective divisors.** We consider now the problem of the determination of the zeta-function. It is known that to determinate the zeta-function of an algebraic function field of genus $g$ defined over a finite field, we just have to study the number $A_i$ of effective divisors of degree $i$ for $i = 0, ..., g-1$. Let us study the asymptotic situation. In this aim, we consider the following asymptotic values defined by Tsfasman in [10], where $A_{\mu g_k}$ denotes the number $A_i$ where $i$ the nearest integer from $\mu g_k$:

$$\Delta(\mu)_{inf}(\mathcal{F}/\mathbb{F}_q) = \liminf_{k \to +\infty} \frac{1}{g_k} \log A_{\mu g_k}$$

$$\Delta(\mu)_{sup}(\mathcal{F}/\mathbb{F}_q) = \limsup_{k \to +\infty} \frac{1}{g_k} \log A_{\mu g_k}$$

If they coincides, we just write:

$$\Delta(\mu)(\mathcal{F}/\mathbb{F}_q) = \lim_{k \to +\infty} \frac{1}{g_k} \log A_{\mu g_k} = \Delta(\mu)_{inf} = \Delta(\mu)_{sup}.$$

Then, we obtain the following result which gives exponential estimates of the number of effective divisors in the particular case of asymptically exact sequences defined previously.

**Theorem 2.8.** *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$ be a sequence of algebraic function fields of increasing genus defined over $\mathbb{F}_q$ such that $\beta_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q^{\frac{r}{2}}-1)$ where $r$ is an integer. Then, the limit $\Delta(\mu)$ exists. Moreover, if we set:*

$$\mu_0 = \frac{q^{\frac{r}{2}}-1}{q^r-1}$$

*then for $\mu \geq \mu_0$, we have:*

$$\Delta(\mu)(\mathcal{F}/\mathbb{F}_q) = \log \frac{q^{\mu+q^{\frac{r}{2}}-1}}{q^r-1} = H - (1-\mu)\log q$$

*and for $0 \leq \mu \leq \mu_0$,*

$$\Delta(\mu)(\mathcal{F}/\mathbb{F}_q) = \log \frac{\mu\big(\frac{q^{\frac{r}{2}}-1}{\mu}+1\big)^{\frac{1}{r}(\mu+q^{\frac{r}{2}}-1)}}{q^{\frac{r}{2}}-1}.$$

*More precisely, we have:*

$$\lim_{k\to+\infty} A_{\mu g_k}^{\frac{1}{g_k}} = \big(\frac{q^{\frac{r}{2}}-1}{\mu}+1\big)^{\frac{\mu}{r}}\big(1-\big(\frac{q^{\frac{r}{2}}-1}{\mu}+1\big)^{-1}\big)^{-\frac{(q^{\frac{r}{2}}-1)}{r}}\big).$$

*Proof.* It is sufficient to apply Theorem 6 in [10] or Proposition 4.1 in [11] with the tower $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_{k\geq 1}$. Then, for the last quantity, we directly apply Theorem 4.1 in [11] with this same tower $\mathcal{F}/\mathbb{F}_q$. □

## 3. Examples of asymptotically exact towers

Let us note $\mathbb{F}_{q^2}$ a finite field with $q = p^r$ and $r$ an integer.

3.1. **Sequences $\mathcal{F}/\mathbb{F}_q$ with $\beta_2(F/\mathbb{F}_q) = \frac{1}{2}(q-1)$.** We consider the Garcia-Stichtenoth's tower $T_0$ over $\mathbb{F}_{q^2}$ constructed in [5]. Recall that this tower is defined recursively in the following way. We set $F_1 = \mathbb{F}_{q^2}(x_1)$ the rational function field over $\mathbb{F}_{q^2}$, and for $i \geq 1$ we define

$$F_{i+1} = F_i(z_{i+1}),$$

where $z_{i+1}$ satisfies the equation

$$z_{i+1}^q + z_{i+1} = x_i^{q+1},$$

with

$$x_i = \frac{z_i}{x_{i-1}} \text{ for } i \geq 2.$$

We consider the completed Garcia-Stichtenoth's tower $T_1$ over $\mathbb{F}_{q^2}$ studied in [2] obtained from $T_0$ by adjonction of intermediate steps. Namely we have

$$T_1 : F_{1,0} \subset \cdots \subset F_{i,0} \subset F_{i,1} \subset \cdots \subset F_{i,s} \subset \cdots \subset F_{i,n-1} \subset F_{i+1,0} \subset \cdots$$

where the steps $F_{i,0}$ are the steps $F_i$ of the Garcia-Stichtenoth's tower and where $F_{i,s}$ $(1 \leq s \leq n-1)$ are the intermediate steps.

Let us denote by $g_k$ the genus of $F_k$ in $T_0$, by $g_{k,s}$ the genus of $F_{k,s}$ in $T_1$ and by $B_1(F_{k,s})$ the number of places of degree one of $F_{k,s}$ in $T_1$.

Recall that each extension $F_{k,s}/F_k$ is Galois of degree $p^s$ wih full constant field $\mathbb{F}_{q^2}$. Moreover, we know by [3] that the descent of the definition field of the tower $T_1$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ is possible. More precisely, there exists a tower $T_2$ defined over $\mathbb{F}_q$ given by a sequence:

$$T_2 : G_{1,0} \subset \cdots \subset G_{i,0} \subset G_{i,1} \subset \cdots \subset G_{i,s} \subset \cdots \subset G_{i,n-1} \subset G_{i+1,0} \subset \cdots$$

defined over the constant fied $\mathbb{F}_q$ and related to the tower $T_1$ by

$$F_{k,s} = \mathbb{F}_{q^2} G_{k,s} \quad \text{for all } k \text{ and } s,$$

namely $F_{k,s}/\mathbb{F}_{q^2}$ is the constant field extension of $G_{k,s}/\mathbb{F}_q$. Let us prove a proposition establishing that the tower $T_2/\mathbb{F}_q$ is asymptotically exact with good density.

**Proposition 3.1.** *Let $q = p^r$. For any integer $k \geq 1$, for any integer $s$ such that $s = 0, 1, ..., r$, the algebraic function field $G_{k,s}/\mathbb{F}_p$ in the tower $T_2$ has a genus $g(G_{k,s}) = g_{k,s}$ with $B_1(G_{k,s})$ places of degree one, $B_2(G_{k,s})$ places of degree two such that:*

1. *$G_k \subseteq G_{k,s} \subseteq G_{k+1}$ with $G_{k,0} = G_k$ and $G_{k+1,0} = G_{k+1}$.*
2. *$g(G_{k,s}) \leq \frac{g(G_{k+1})}{p^{r-s}} + 1$ with $g(G_{k+1}) = g_{k+1} \leq q^{k+1} + q^k$ .*
3. *$B_1(G_{k,s}) + 2B_2(G_{k,s}) \geq (q^2-1)q^{k-1}p^s$.*
4. *$\beta_2(T_2/\mathbb{F}_q) = \lim_{g_{k,s} \rightarrow +\infty} \frac{B_2(G_{k,s}/\mathbb{F}_q)}{g_k} = \frac{1}{2}(q-1)$.*
5. *$d(T_2/\mathbb{F}_q) = \lim_{l \rightarrow +\infty} \frac{g(G_l)}{g(G_{l+1})} = \frac{1}{p}$ where $g(G_l)$ and $g(G_{l+1})$ denote the genus of two consecutive algebraic function fields in $T_2$.*

*Proof.* The property 1) follows directly from Theorem 4.3 in [3]. Moreover, by Theorem 2.2 in [2], we have $g(F_{k,s}) \leq \frac{g(F_{k+1})}{p^{r-s}} + 1$ with $g(F_{k+1}) = g_{k+1} \leq q^{k+1} + q^k$ . Then, as the algebraic function field $F_{k,s}$ is a constant field extension of $G_{k,s}$, for any integer $k$ and $s$ the algebraic function fields $F_{k,s}$ and $G_{k,s}$ have the same genus. So, the inequality satisfied by the genus $g(F_{k,s})$ is also true for the genus $g(G_{k,s})$. Moreover, the number of places of degree one $B_1(F_{k,s}/\mathbb{F}_{q^2})$ of $F_{k,s}/\mathbb{F}_{q^2}$ is such that $B_1(F_{k,s}/\mathbb{F}_{q^2}) \geq (q^2-1)q^{k-1}p^s$. Then, as the algebraic function field $F_{k,s}$ is a constant field extension of $G_{k,s}$ of degree 2, it is clear that for any integer $k$ and $s$, we have $B_1(G_{k,s}/\mathbb{F}_p) + 2B_2(G_{k,s}/\mathbb{F}_p) \geq (q^2-1)q^{k-1}p^s$. Moreover, we know that for any integer $k \geq 1$, the number of places of degree one $B_1(G_{k,s}/\mathbb{F}_q)$ of $G_{k,s}/\mathbb{F}_q$ corresponds at most to the number of places of degree one $B_1(F_{k,s}/\mathbb{F}_{q^2})$ of $F_{k,s}/\mathbb{F}_{q^2}$

which are totally ramified in the tower $T_1$ by [5]. Hence, for any integer $k$ and $s$, we have $B_1(G_{k,s}/\mathbb{F}_q) \leq q+1$ and so $\beta_1(T_2/\mathbb{F}_q) = 0$. Moreover, $B_1(G_{k,s}/\mathbb{F}_q) + 2B_2(G_{k,s}/\mathbb{F}_p) = B_1(F_{k,s}/\mathbb{F}_{q^2})$ and as by [5], $\beta_1(T_1/\mathbb{F}_{q^2}) = A(q^2)$, we have $\beta_2(T_2/\mathbb{F}_p) = \frac{1}{2}(q-1)$.

□

### 3.2. **Sequences $\mathcal{F}/\mathbb{F}_q$ with $\beta_4(\mathcal{F}/\mathbb{F}_q) = \frac{1}{4}(q^2-1)$.**

3.2.1. *The descent on the definition field $\mathbb{F}_p$ of a Garcia-Stichtenoth tower defined over $\mathbb{F}_{q^2}$.* Now, we are interested in searching the descent of the definition field of the tower $T_1$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$ if it is possible. In fact, we can not establish a general result but we can prove that it is possible in the case of caracteristic 2 which is given by the following result.

**Proposition 3.2.** *Let $p = 2$. If $q = p^2$, the descent of the definition field of the tower $T_1$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$ is possible. More precisely, there exists a tower $T_3$ defined over $\mathbb{F}_p$ given by a sequence:*

$$T_3 = H_{1,0} \subseteq H_{1,1} \subseteq H_{2,0} \subseteq H_{2,1} \subseteq ...$$

*defined over the constant fied $\mathbb{F}_p$ and related to the towers $T_1$ and $T_2$ by*

$$F_{k,s} = \mathbb{F}_{q^2} H_{k,s} \quad for\ all\ k\ and\ s = 0, 1,$$

$$G_{k,s} = \mathbb{F}_q H_{k,s} \quad for\ all\ k\ and\ s = 0, 1,$$

*namely $F_{k,s}/\mathbb{F}_{q^2}$ is the constant field extension of $G_{k,s}/\mathbb{F}_q$ and $H_{k,s}/\mathbb{F}_q$ and $G_{k,s}/\mathbb{F}_q$ is the constant field extension of $H_{k,s}/\mathbb{F}_p$.*

*Proof.* Let $x_1$ be a transcendent element over $\mathbb{F}_2$ and let us set

$$H_1 = \mathbb{F}_2(x_1), G_1 = \mathbb{F}_4(x_1), F_1 = \mathbb{F}_{16}(x_1).$$

We define recursively for $k \geq 1$

(1) $z_{k+1}$ such that $z_{k+1}^4 + z_{k+1} = x_k^5$,
(2) $t_{k+1}$ such that $t_{k+1}^2 + t_{k+1} = x_k^5$
(or alternatively $t_{k+1} = z_{k+1}(z_{k+1}+1)$),
(3) $x_k = z_k/x_{k-1}$ if $k > 1$ ($x_1$ is yet defined),
(4) $H_{k,1} = H_{k,0}(t_{k+1}) = H_k(t_{k+1})$, $H_{k+1,0} = H_{k+1} = H_k(z_{k+1})$, $G_{k,1} = G_{k,0}(t_{k+1}) = G_k(t_{k+1})$, $G_{k+1,0} = G_{k+1} = G_k(z_{k+1})$, $F_{k,1} = F_{k,0}(t_{k+1}) = F_k(t_{k+1})$, $F_{k+1,0} = F_{k+1} = F_k(z_{k+1})$.

By [3], the tower $T_1 = (F_{k,i})_{k\geq 1, i=0,1}$ is the densified Garcia-Stichtenoth's tower over $\mathbb{F}_{16}$ and the two other towers $T_2$ and $T_3$ are respectively the descent of $T_1$ over $\mathbb{F}_4$ and over $\mathbb{F}_2$. □

**Proposition 3.3.** *Let $q = p^2 = 4$. For any integer $k \geq 1$, for any integer $s$ such that $s = 0, 1, 2$, the algebraic function field $H_{k,s}/\mathbb{F}_p$ in the tower $T_3$ has a genus $g(H_{k,s}) = g_{k,s}$ with $B_1(H_{k,s})$ places of degree one, $B_2(H_{k,s})$ places of degree two and $B_4(H_{k,s})$ places of degree 4 such that:*

(1) $H_k \subseteq H_{k,s} \subseteq H_{k+1}$ *with* $H_{k,0} = H_k$.
(2) $g(H_{k,s}) \leq \frac{g(H_{k+1})}{p^{r-s}} + 1$ *with* $g(H_{k+1}) = g_{k+1} \leq q^{k+1} + q^k$ .
(3) $B_1(H_{k,s}) + 2B_2(H_{k,s}) + 4B_4(H_{k,s}) \geq (q^2 - 1)q^{k-1}p^s$.
(4) $\beta_4(T_3/\mathbb{F}_p) = \lim_{g_{k,s}\rightarrow+\infty} \frac{B_4(H_{k,s}/\mathbb{F}_p)}{g_k} = \frac{1}{4}(p^2 - 1)$.
(5) $d(T_3/\mathbb{F}_p) = \lim_{l\rightarrow+\infty} \frac{g(H_l)}{g(H_{l+1})} = \frac{1}{2}$ *where* $g(H_l)$ *and* $g(H_{l+1})$ *denote the genus of two consecutive algebraic function fields in* $T_3$.

*Proof.* The property 1) follows directly from Proposition 3.2. Moreover, by Theorem 2.2 in [2], we have $g(F_{k,s}) \leq \frac{g(F_{k+1})}{p^{r-s}} + 1$ with $g(F_{k+1}) = g_{k+1} \leq q^{k+1}+q^k$ . Then, as the algebraic function field $F_{k,s}$ is a constant field extension of $H_{k,s}$, for any integer $k$ and $s$ the algebraic function fields $F_{k,s}$ and $H_{k,s}$ have the same genus. So, the inequality satisfied by the genus $g(F_{k,s})$ is also true for the genus $g(H_{k,s})$. Moreover, the number of places of degree one $B_1(F_{k,s}/\mathbb{F}_{q^2})$ of $F_{k,s}/\mathbb{F}_{q^2}$ is such that $B_1(F_{k,s}/\mathbb{F}_{q^2}) \geq (q^2-1)q^{k-1}p^s$. Then, as the algebraic function field $F_{k,s}$ is a constant field extension of $H_{k,s}$ of degree 4, it is clear that for any integer $k$ and $s$, we have $B_1(H_{k,s}/\mathbb{F}_p)+2B_2(H_{k,s}/\mathbb{F}_p)+4B_4(H_{k,s}/\mathbb{F}_p) \geq (q^2-1)q^{k-1}p^s$. Moreover, we know that for any integer $k \geq 1$, the number of places of degree one $B_1(G_{k,s}/\mathbb{F}_q)$ of $G_{k,s}/\mathbb{F}_q$ corresponds at most to the number of places of degree one $B_1(F_{k,s}/\mathbb{F}_{q^2})$ of $F_{k,s}/\mathbb{F}_{q^2}$ which are totally ramified in the tower $T_1$ by [5]. Hence, for any integer $k$ and $s$, we have $B_1(G_{k,s}/\mathbb{F}_q) \leq q + 1$ and so $\beta_1(T_2/\mathbb{F}_q) = 0$. Then, as the algebraic function field $G_{k,s}$ is a constant field extension of $H_{k,s}$ of degree 2, it is clear that for any integer $k$ and $s$, we have $B_1(H_{k,s}/\mathbb{F}_p)+2B_2(H_{k,s}/\mathbb{F}_p) \leq B_1(G_{k,s}/\mathbb{F}_q)$ and so $\beta_1(T_3/\mathbb{F}_p) = \beta_2(T_3/\mathbb{F}_p) = 0$. Moreover, $B_1(H_{k,s}/\mathbb{F}_p) + 2B_2(H_{k,s}/\mathbb{F}_p) + 4B_4(H_{k,s}/\mathbb{F}_p) = B_1(F_{k,s}/\mathbb{F}_{q^2})$ and as by [5], $\beta_1(T_1/\mathbb{F}_{q^2}) = A(q^2)$, we have $\beta_4(T_3/\mathbb{F}_p) = A(p^4) = p^2 - 1$. □

**Corollary 3.4.** *Let $T_3/\mathbb{F}_2 = (H_{k,s}/\mathbb{F}_2)_{k\in\mathbb{N},s=0,1,2}$ be the tower defined above. Then the tower $T_3/\mathbb{F}_2$ is an asymptotically exact sequence of algebraic function fields defined over $\mathbb{F}_2$ with a maximal density (for a tower).*

*Proof.* It follows from (4) of Proposition 3.1. □

## References

[1] Stéphane Ballet. Quasi-optimal algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree 13, 14, and 15. *Journal of Pure and Applied Algebra*, 171:149–164, 2002.

[2] Stéphane Ballet. Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of $\mathbb{F}_q$. *Finite Fields and Their Applications*, 9:472–478, 2003.

[3] Stéphane Ballet, Dominique Le Brigand, and Robert Rolland. On an application of the definition field descent of a tower of function fields. In *Proceedings of the Conference Arithmetic, Geometry and Coding Theory (AGCT 2005)*, volume 21, pages 187–203. Société Mathématique de France, sér. Séminaires et Congrès, 2009.

[4] Stéphane Ballet and Robert Rolland. Asymptotic bounds for the tensor rank of the multiplication in finite extensions of $\mathbb{F}_2$. *Preprint IML*, 12, 2008.

[5] Arnaldo Garcia and Henning Stitchtenoth. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Inventiones Mathematicae*, 121:211–222, 1995.

[6] Gilles Lachaud and Mireille Martin-Deschamps. Nombre de points des jacobiennes sur un corps finis. *Acta Arithmetica*, 56(4):329–340, 1990.

[7] Michael Rosenbloom and Michael Tsfasman. Multiplicative lattices in global fields. *Inventiones Mathematicae*, 17:53–54, 1983.

[8] Jean-Pierre Serre. The number of rationnal points on curves over finite fields, 1983. Notes by E. Bayer, Princeton Lectures.

[9] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Number 314 in Lectures Notes in Mathematics. Springer-Verlag, 1993.

[10] Michael Tsfasman. Some remarks on the asymptotic number of points. In H. Stichtenoth and M.A. Tsfasman, editors, *Coding Theory and Algebraic Geometry*, volume 1518 of *Lecture Notes in Mathematics*, pages 178–192, Berlin, 1992. Springer-Verlag. Proceedings of AGCT-3 conference, June 17-21, 1991, Luminy.

[11] Michael Tsfasman and Serguei Vladut. Asymptotic properties of zeta-functions. *Journal of Mathematical Sciences*, 84(5):1445–1467, 1997.

[12] Serguei Vladut. An exhaustion bound for algebraic-geometric modular codes. *Problems of Information Transmission*, 23:22–34, 1987.

[13] Serguei Vladut and Vladimir Drinfeld. Number of points of an algebraic curve. *Funktsional Anal i Prilozhen*, 17:53–54, 1983.

Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France

*E-mail address*: `ballet@iml.univ-mrs.fr`

Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France

*E-mail address*: `robert.rolland@acrypta.fr`